ID: 338146
Cookbook: browseurl.jbs
Time: 18:01:06
Date: 11/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

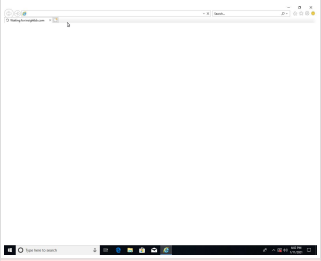
Analysis Report http://insightbb.com/

Overview

General Information

Sample URL:	http://insightbb.com/
Analysis ID:	338146

Most interesting Screenshot:



Errors

URL not reachable

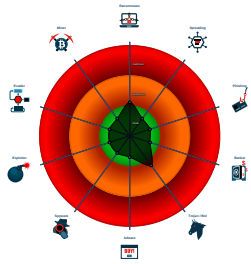
Detection

Score:	0
Range:	0 - 100
Whitelisted:	false
Confidence:	60%

Signatures

Tries to connect to HTTP servers, b…

Classification



Analysis Advice

All HTTP servers contacted by the sample do not answer. Likely the sample is an old dropper which does no longer work

Joe Sandbox was unable to browse the URL (domain or webserver down or HTTPS issue), try to browse the URL again later

Startup

- **System is w10x64**
- iexplore.exe (PID: 6796 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6844 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6796 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

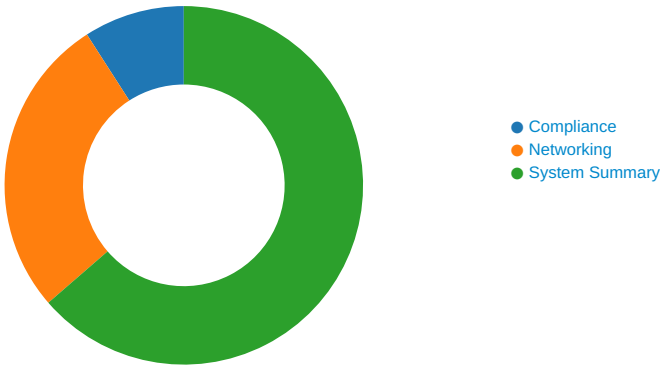
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



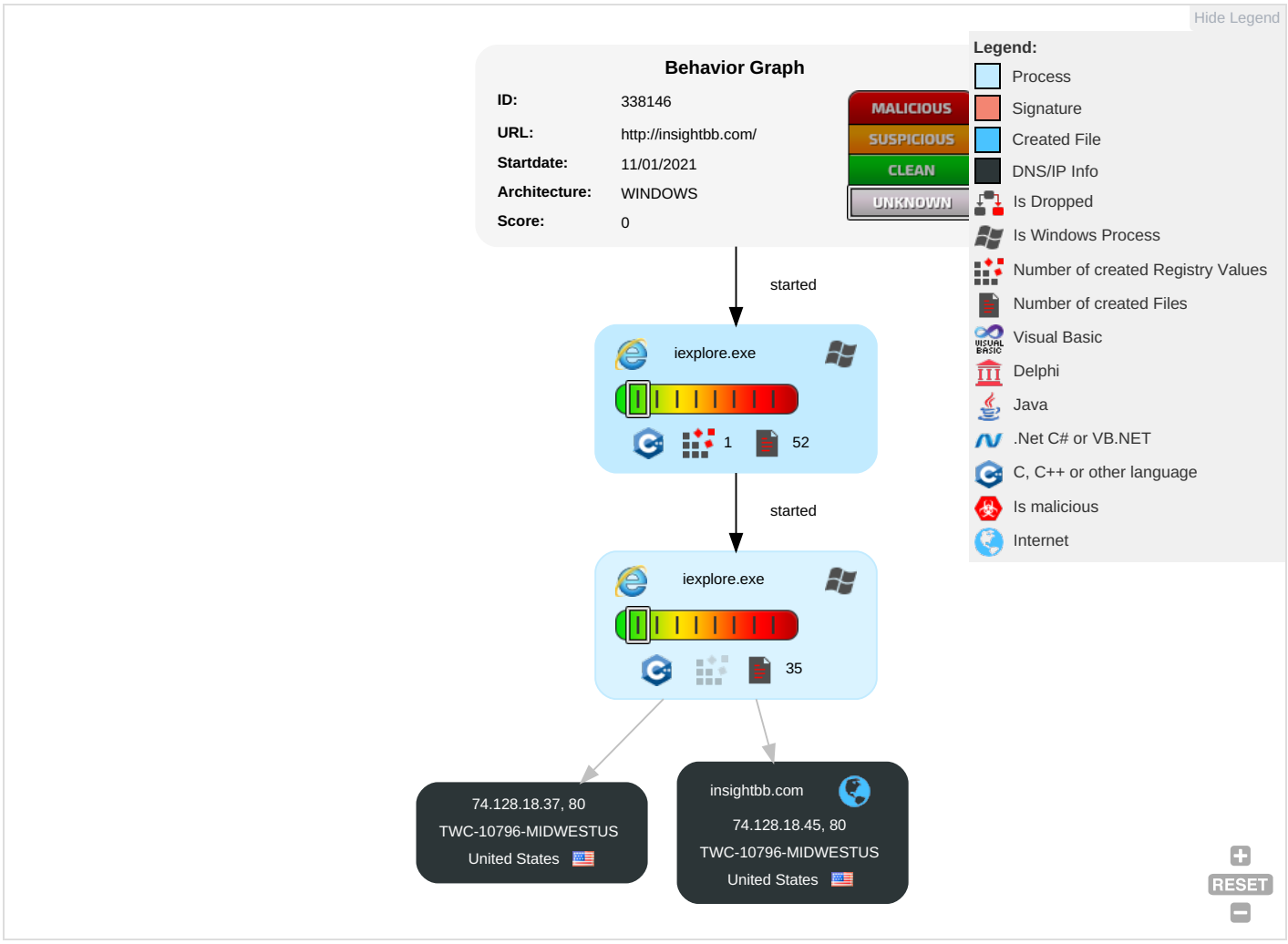
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

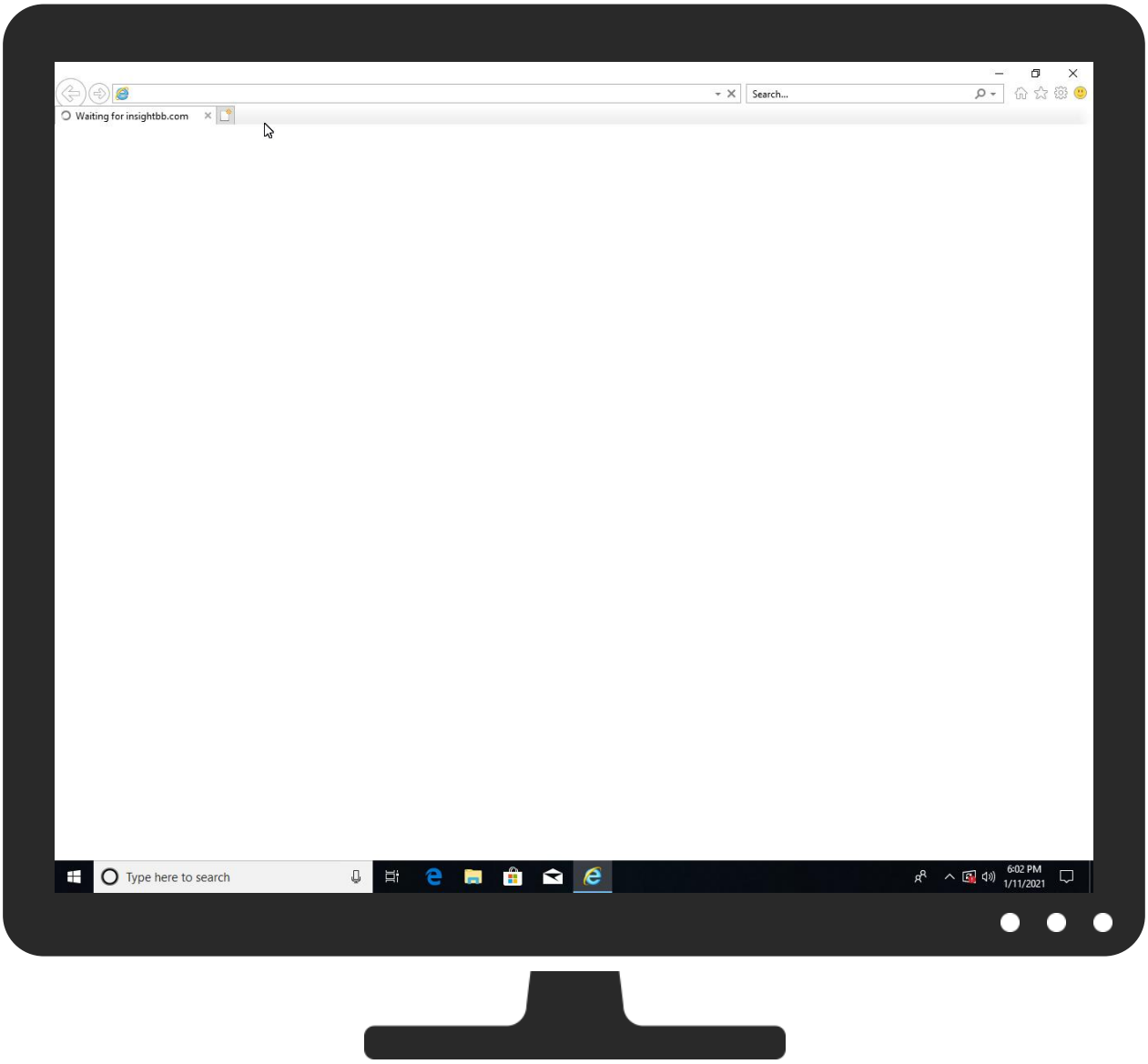
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
http://insightbb.com/	0%	Virustotal		Browse
http://insightbb.com/	0%	Avira URL Cloud	safe	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
insightbb.com	74.128.18.45	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://insightbb.com/	~DFF4C9C92D8875D8BB.TMP.1.dr	false		high
http://insightbb.com/Root	{B2EF0FDC-542E-11EB-90EB-ECF4BBEA1588}.dat.1.dr	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
74.128.18.45	unknown	United States		10796	TWC-10796-MIDWESTUS	false
74.128.18.37	unknown	United States		10796	TWC-10796-MIDWESTUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338146
Start date:	11.01.2021
Start time:	18:01:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	browseurl.jbs
Sample URL:	http://insightbb.com/

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	9
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	UNKNOWN
Classification:	unknown0.win@3/11@2/2
Cookbook Comments:	• Adjust boot time • Enable AMSI • **URL browsing timeout or error**
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 104.42.151.234, 88.221.62.148, 51.104.139.180, 92.122.213.247, 92.122.213.194, 152.199.19.161, 52.155.217.156 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, ie9comview.vo.msecnd.net, displaycatalog.md.mp.microsoft.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, go.microsoft.com, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus16.cloudapp.net, cs9.wpc.v0cdn.net
Errors:	• URL not reachable

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{B2EF0FDA-542E-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	30296
Entropy (8bit):	1.8567196798588723
Encrypted:	false
SSDEEP:	192:rxZmZ02D9WXteifwYuVzMAGVBpUVDvsfXYZVjX:r3CjDU9PUqnnuV6k5
MD5:	EDE61F120C3677B4ABE24B9FF40D8BF4
SHA1:	8237642C786A64A081AA5CC7FDB11DA929C3C569
SHA-256:	77D1E57E5EE4167D769FB2A9AE899C3A915105C50A133365A2AF3687AB0B45C6
SHA-512:	2E8F692C544FE426432784528FE527E9E377685BF3D303AF0CDCCB90AFD90574759491CF3E77697A7B204AEC879B20BE3A3617F3CF19DE22FA5BA03A97EC27F
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{B2EF0FDC-542E-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	23640
Entropy (8bit):	1.6391535210503922
Encrypted:	false
SSDEEP:	48:Iwd7GcprwjGwpaM7G4pQAGrapbS1rGQpBKGHHpcqsTGUp8HGzYpm7MYGopeFuGhh:rXZcQl6eBS1FjR2qkWlMAYU1h
MD5:	B3253CCF40F61719D43285E53A0F2A72
SHA1:	83CCEC61037DF0197CFA821FDF7DA0C6B62C84CB
SHA-256:	90D79245C0686663A229CFA457635C77063C30024EF5CBBF49F437E5146EDD52
SHA-512:	6CB93ED86AB8AF5B9787748B7AC9F2DD27DBD102CE7B71363A8848BBEC64D9EB17438E133BE62F3EFD6E148DA16B0A0EBD24C0DC9A9B5C7C464E171B4C239 447
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{BD779198-542E-11EB-90EB-ECF4BBEA1588}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.566168126534175
Encrypted:	false
SSDEEP:	48:IwsGcpr1jGwpaEG4pQgGrapbSIxrGQpKKG7HpRTsTGIpG:rwZLQ06+BSIxFAlTT4A
MD5:	C6AD764761438F56C6AFB51F8D4BB1EB
SHA1:	E049BCCC91E7E04706C8BC94BC2748458B1045E1
SHA-256:	2C99FC84D04D62BDA7D9BE760FFA87C5DA0D892F6B3B3A89484F4B1DE24F6EBB
SHA-512:	3A75C421285FDAC61F925D05F5DFEB2D9C0045557EA526A562A19F4A29F40846352BCE7CF8E8F0E306C356650254DAE2386BCF3F36762D7233C9BE9019091EE
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{BD779198-542E-11EB-90EB-ECF4BBEA1588}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vIlJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493AC6D
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=0
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMoreInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/errorPageStrings.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9026IKNJ\errorPageStrings[1]	
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";..../used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CS6IXJW6\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.su bstring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var pound Index = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OR0WKIO1\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
Reputation:	low
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #00 0000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Temp\~DF677BE9D68FA659FB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13029
Entropy (8bit):	0.47958646381791603
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loLS9loLC9lWLBiLiWA0maiLimzEmYmCmaCm3:kBqoIx3wLwLW
MD5:	729F4EC0119B3B56554A0BD9CD077978
SHA1:	B49F2B7D7487CFC1EAE324AB22C433589B06DF88
SHA-256:	4B3DD650A69F439310145B23166CFB101D2C1AC488B370C51CC7A24027F852AB
SHA-512:	E9223D05AC2E61A7DF998682E831B32FDF0C76398280210B155789ED73C23C312E9892FA3355B7D65AD424F8890F84B7376F078B3E3359799144780E31901CB2
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\~DF677BE9D68FA659FB.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFAC921340B91BE7BE.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25441
Entropy (8bit):	0.27918767598683664
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRx/9lRJ9lTb9lTb9lSSU9lSSU9laAa/9laA:kBqoxxJhHWSVSEab
MD5:	AB889A32AB9ACD33E816C2422337C69A
SHA1:	1190C6B34DED2D295827C2A88310D10A8B90B59B
SHA-256:	4D6EC54B8D244E63B0F04FBE2B97402A3DF722560AD12F218665BA440F4CEFDA
SHA-512:	BD250855747BB4CEC61814D0E44F810156D390E3E9F120A12935EFDF80ACA33C4777AD66257CCA4E4003FEF0741692894980B9298F01C4CDD2D8A9C7BB522FB
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFF4C9C92D8875D8BB.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	34345
Entropy (8bit):	0.346528610406187
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwVz9lwVz9l2VF9l2VFk:kBqoxKAuvScS+yU+X7I7gF+
MD5:	50A46C9A5C79BD00659F86757DD5E037
SHA1:	37620FA6806036CAD443410ED61B11D84A5FC96C
SHA-256:	DD70A83B8C398EC59BD3951EB0BF5E0E3FA481613BD0142F53CC1DFF4C199075
SHA-512:	2A6EF66D567B777D3AFB5A68985589815663BEF43932FAF368150FD03E0B99069F2E6B40987D9DA62947E043CAF8A3FD1ABBEAD88705041A87AF8794A2EB18DA
Malicious:	false
Reputation:	low
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

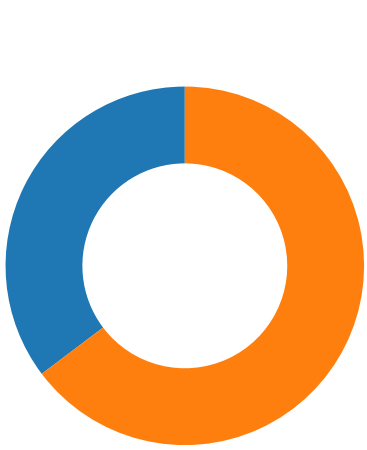
No static file info

Network Behavior

Network Port Distribution

Total Packets: 51

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:01:53.965090990 CET	49729	80	192.168.2.4	74.128.18.45
Jan 11, 2021 18:01:53.965922117 CET	49730	80	192.168.2.4	74.128.18.45
Jan 11, 2021 18:01:54.972388983 CET	49729	80	192.168.2.4	74.128.18.45
Jan 11, 2021 18:01:54.973612070 CET	49730	80	192.168.2.4	74.128.18.45
Jan 11, 2021 18:01:56.972750902 CET	49729	80	192.168.2.4	74.128.18.45
Jan 11, 2021 18:01:56.988253117 CET	49730	80	192.168.2.4	74.128.18.45
Jan 11, 2021 18:02:00.977680922 CET	49737	80	192.168.2.4	74.128.18.37
Jan 11, 2021 18:02:01.006335020 CET	49738	80	192.168.2.4	74.128.18.37
Jan 11, 2021 18:02:01.973117113 CET	49737	80	192.168.2.4	74.128.18.37
Jan 11, 2021 18:02:02.019911051 CET	49738	80	192.168.2.4	74.128.18.37
Jan 11, 2021 18:02:04.004403114 CET	49737	80	192.168.2.4	74.128.18.37
Jan 11, 2021 18:02:04.035660028 CET	49738	80	192.168.2.4	74.128.18.37
Jan 11, 2021 18:02:08.194236994 CET	49742	80	192.168.2.4	74.128.18.45
Jan 11, 2021 18:02:09.223571062 CET	49742	80	192.168.2.4	74.128.18.45
Jan 11, 2021 18:02:11.223683119 CET	49742	80	192.168.2.4	74.128.18.45
Jan 11, 2021 18:02:15.225976944 CET	49745	80	192.168.2.4	74.128.18.37
Jan 11, 2021 18:02:16.239945889 CET	49745	80	192.168.2.4	74.128.18.37
Jan 11, 2021 18:02:18.255547047 CET	49745	80	192.168.2.4	74.128.18.37

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:01:48.537352085 CET	49910	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:01:48.585350037 CET	53	49910	8.8.8.8	192.168.2.4
Jan 11, 2021 18:01:50.949341059 CET	55854	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:01:50.997523069 CET	53	55854	8.8.8.8	192.168.2.4
Jan 11, 2021 18:01:52.067065001 CET	64549	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:01:52.115281105 CET	53	64549	8.8.8.8	192.168.2.4
Jan 11, 2021 18:01:52.753319025 CET	63153	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:01:52.811464071 CET	53	63153	8.8.8.8	192.168.2.4
Jan 11, 2021 18:01:53.444315910 CET	52991	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:01:53.492336988 CET	53	52991	8.8.8.8	192.168.2.4
Jan 11, 2021 18:01:53.767503023 CET	53700	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:01:53.949974060 CET	53	53700	8.8.8.8	192.168.2.4
Jan 11, 2021 18:01:54.735121965 CET	51726	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:01:54.791621923 CET	53	51726	8.8.8.8	192.168.2.4
Jan 11, 2021 18:01:56.060774088 CET	56794	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:01:56.109112978 CET	53	56794	8.8.8.8	192.168.2.4
Jan 11, 2021 18:01:57.226811886 CET	56534	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:01:57.274945021 CET	53	56534	8.8.8.8	192.168.2.4
Jan 11, 2021 18:01:58.366658926 CET	56627	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:01:58.417566061 CET	53	56627	8.8.8.8	192.168.2.4
Jan 11, 2021 18:01:59.726530075 CET	56621	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:01:59.777445078 CET	53	56621	8.8.8.8	192.168.2.4
Jan 11, 2021 18:02:00.894500017 CET	63116	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 11, 2021 18:02:00.942497969 CET	53	63116	8.8.8.8	192.168.2.4
Jan 11, 2021 18:02:02.032020092 CET	64078	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:02:02.083156109 CET	53	64078	8.8.8.8	192.168.2.4
Jan 11, 2021 18:02:03.236465931 CET	64801	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:02:03.284668922 CET	53	64801	8.8.8.8	192.168.2.4
Jan 11, 2021 18:02:04.799345016 CET	61721	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:02:04.847397089 CET	53	61721	8.8.8.8	192.168.2.4
Jan 11, 2021 18:02:13.067286968 CET	51255	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:02:13.118238926 CET	53	51255	8.8.8.8	192.168.2.4
Jan 11, 2021 18:02:18.372941017 CET	61522	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:02:18.433882952 CET	53	61522	8.8.8.8	192.168.2.4
Jan 11, 2021 18:02:22.297149897 CET	52337	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:02:22.353491068 CET	53	52337	8.8.8.8	192.168.2.4
Jan 11, 2021 18:02:22.746351004 CET	55046	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:02:22.805042028 CET	53	55046	8.8.8.8	192.168.2.4
Jan 11, 2021 18:02:23.424632072 CET	49612	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:02:23.472673893 CET	53	49612	8.8.8.8	192.168.2.4
Jan 11, 2021 18:02:23.742291927 CET	55046	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:02:23.790430069 CET	53	55046	8.8.8.8	192.168.2.4
Jan 11, 2021 18:02:24.428121090 CET	49612	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:02:24.476248980 CET	53	49612	8.8.8.8	192.168.2.4
Jan 11, 2021 18:02:24.756225109 CET	55046	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:02:24.804513931 CET	53	55046	8.8.8.8	192.168.2.4
Jan 11, 2021 18:02:25.443759918 CET	49612	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:02:25.491589069 CET	53	49612	8.8.8.8	192.168.2.4
Jan 11, 2021 18:02:26.857594013 CET	55046	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:02:26.905591965 CET	53	55046	8.8.8.8	192.168.2.4
Jan 11, 2021 18:02:27.444041014 CET	49612	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:02:27.491988897 CET	53	49612	8.8.8.8	192.168.2.4
Jan 11, 2021 18:02:29.769109964 CET	49285	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:02:29.825440884 CET	53	49285	8.8.8.8	192.168.2.4
Jan 11, 2021 18:02:30.346611977 CET	50601	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:02:30.405796051 CET	53	50601	8.8.8.8	192.168.2.4
Jan 11, 2021 18:02:30.869676113 CET	55046	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:02:30.917637110 CET	53	55046	8.8.8.8	192.168.2.4
Jan 11, 2021 18:02:30.979654074 CET	60875	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:02:31.030450106 CET	53	60875	8.8.8.8	192.168.2.4
Jan 11, 2021 18:02:31.450377941 CET	56448	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:02:31.459826946 CET	49612	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:02:31.506617069 CET	53	56448	8.8.8.8	192.168.2.4
Jan 11, 2021 18:02:31.516278982 CET	53	49612	8.8.8.8	192.168.2.4
Jan 11, 2021 18:02:32.138701916 CET	59172	53	192.168.2.4	8.8.8.8
Jan 11, 2021 18:02:32.189471960 CET	53	59172	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 11, 2021 18:01:53.767503023 CET	192.168.2.4	8.8.8.8	0x7ea3	Standard query (0)	insightbb.com	A (IP address)	IN (0x0001)
Jan 11, 2021 18:02:22.297149897 CET	192.168.2.4	8.8.8.8	0xa9f1	Standard query (0)	insightbb.com	A (IP address)	IN (0x0001)

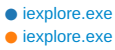
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 11, 2021 18:01:53.949974060 CET	8.8.8.8	192.168.2.4	0x7ea3	No error (0)	insightbb.com		74.128.18.45	A (IP address)	IN (0x0001)
Jan 11, 2021 18:01:53.949974060 CET	8.8.8.8	192.168.2.4	0x7ea3	No error (0)	insightbb.com		74.128.18.37	A (IP address)	IN (0x0001)
Jan 11, 2021 18:02:22.353491068 CET	8.8.8.8	192.168.2.4	0xa9f1	No error (0)	insightbb.com		74.128.18.45	A (IP address)	IN (0x0001)
Jan 11, 2021 18:02:22.353491068 CET	8.8.8.8	192.168.2.4	0xa9f1	No error (0)	insightbb.com		74.128.18.37	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: iexplore.exe PID: 6796 Parent PID: 800

General

Start time:	18:01:51
Start date:	11/01/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff7e9fa0000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6844 Parent PID: 6796

General

Start time:	18:01:52
Start date:	11/01/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6796 CREDAT:17410 /prefetch:2
Imagebase:	0x1010000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly